NASA
Technical
Paper
2409
c.2
April 1985

Reliability Bounds for Fault-Tolerant Systems With Competing Responses to Component Failures

Larry D. Lee

NASA

NASA Technical Paper 2409

1985

Reliability Bounds for Fault-Tolerant Systems With Competing Responses to Component Failures

Larry D. Lee

Langley Research Center
Hampton, Virginia

National Aeronautics and Space Administration

Scientific and Technical Information Branch

SUMMARY

This paper establishes bounds on the probability of system failure for fault-tolerant systems of the type used, for example, in aviation control. Event series leading to system failure are assumed to follow a semi-Markov model in which the potential sojourn times associated with component failures have exponential distributions and those associated with system responses have distributions with unspecified form. A product form of the bounds is derived by using a model that provides for multiple competing system responses to component failures. The general form of the bounds is expressed in terms of integral factors that depend on component failure rates and the distributions of system response times. The bounds are also expressed in terms of percentiles, conditional mean response times, and certain transition probabilities. The accuracy of the bounds is discussed both analytically and in terms of an example system.

1. INTRODUCTION

In recent years, the desire to improve performance, reliability, and safety of commercial and military aircraft systems has led to the increased use of fault-tolerant hardware and software control systems. Some control systems now employ tests to detect and identify failed components and, if failures are identified, the system may reconfigure to exclude information provided by failed components. The techniques for doing this (Montgomery, 1975; Smith et al., 1977; and Willsky, 1976) are often based on hardware duplication of like components with comparison monitoring for failure detection, voting or averaging to mask errors from failed components, and regrouping and repeated comparison for failure identification; also, reconfiguration may take the form of switchovers to spare components or switchovers to operational components.

Early recognition that combinatorial assessment methods would not readily account for the effect on system reliability of such state-dependent system responses has led to the use of multistate point process models. Several automated semi-Markov and nonhomogeneous Markov models and the associated solution techniques, which have been proposed over the last several years, are surveyed and discussed by Geist and Trivedi, 1983, in terms of design limitations imposed by model assumptions, efficiency and accuracy of the solution techniques employed, and the usefulness of the types of solutions obtained.

Although some authors suggest direct computational methods (Ng and Avižienis, 1976), or approximate methods based on state aggregation techniques in detailed fault-handling models (Stiffler et al., 1979), White, 1984, suggests upper and lower bounds for system unreliability. The framework from which he derives the bounds is a semi-Markov model in which component failure times have exponential distributions and system response times have distributions with unspecified form. His bounds take a product form, with one set of factors depending on information concerning component failure rates and another set depending, in addition, on the means and variances of the response times.

In this paper the bounds given by White, 1984, are generalized to a model that provides for competing system responses to component failures. The model describes

a system's history, which consists of a series of states entered over a period of time together with the time intervals between state changes. Entrance into a state may correspond to the occurrence of a component failure or to the occurrence of a system response to previously failed components. Competing responses are often of types such as detecting and deactivating previously failed components or activating spare components. The assumed model is semi-Markov. in which the potential (possible) sojourn times associated with component failures have exponential distributions and those associated with system responses have distributions with unspecified form.

Information concerning system response times may be available from experimental fault injection studies (Lala and Smith, 1983) or from analytical derivations of the response time distributions, as determined from specifications of sequential statistical tests that are often employed in system design (Walker, 1980).

In section 3 a product form of the bounds is derived which has integral factors that depend on component failure rates and the distributions of system response times. This form permits substituting sample cumulative distributions and eliminates the need for certain intermediate stages of data analysis, such as checking the adequacy of assumed parametric forms. The simpler form given in section 4 may be useful when minimal information is available in the form of conditional mean response times, percentiles, and certain transition probabilities. To reduce further the information needed, certain nonparametric classes of response time distributions may be employed, as discussed in section 5.

2. THE MODEL

In the context of a particular application, a system state is a vector having elements that specify the number of operational components, the status of system response, and the current system configuration. It is convenient to label the system states simply as $\{1, 2, \ldots, k\}$. A certain subset R corresponds to states entered as a result of system responses to component failures, and the remaining set $\bar{R}$ corresponds to states entered when components fail. As illustrated in section 6, it is possible for some element of R to correspond to an absorbing state (system failure).

A system's history consists of a series of states $z_0, z_1, \ldots, z_n$ entered over a period of time together with the sojourn times (time intervals between state changes) $u_1, u_2, \ldots, u_n$. Typically, the initial state z_0 is a fully operational system state and z_1 is entered when some component fails. The system may enter z_2 as a result of another component failure or as a result of system response to the first failure, and so on, giving a series of states in R and $\bar{R}$. Successive responses may result from failure detection and subsequent deactivation of a failed component. Competing responses arise, for example when two components, say A and B, have failed and the potential responses are of types such as deactivate A versus deactivate B or activate the spare A versus deactivate the failed active unit B.

If the process is semi-Markov, then the random variables $Z_0, Z_1, \ldots, Z_n$ follow a Markov chain and the sojourn times $U_1, U_2, \ldots, U_n$ are conditionally independent, given a particular series of state changes. The usual model specification (Lagakos et al., 1978) is given by the initial and transition probabilities and by the conditional distributions of the sojourn times as follows:

$$\theta(i) = P(Z_0 = i) \qquad \theta(i,j) = P(Z_{m+1} = j \mid Z_m = i)$$

$$Q(x;i,j) = P(U_{m+1} \leqq x \mid Z_m = i, Z_{m+1} = j)$$

Suppose that the system enters state $z_{m-1} = i$ at the m-1st epoch. Let $T(i,\ell)$ ($\ell = 1, 2, \ldots, k$) denote the potential (possible) sojourn times associated with the states $\ell = 1, 2, \ldots, k$. Then, the system enters state j only if $T(i,j)$ is the smallest of the potential sojourn times. The time between the m-1st and mth epochs is $U_m = \min\{T(i,1), T(i,2), \ldots, T(i,k)\}$. In particular, $\theta(i,j)$ $Q(x;i,j)$ gives the probability that $U_m \leqq x$ and $T(i,j) \leqq \min\{T(i,\ell)\}$, where $\ell \neq j, \ldots,$ given that the current system state is $z_{m-1} = i$.

If the potential sojourn times are independent and have continuous distributions, then

$$\theta(i,j)\, dQ(x;i,j) = \Pi_{\ell \neq j}\, \bar{G}(x;i,\ell)\, dG(x;i,j) \qquad (1)$$

where $\bar{G}(x;i,\ell) = P\{T(i,\ell) > x\}$ represents the survivor functions. As mentioned earlier, the potential sojourn times $T(i,\ell)$, $\ell \in \bar{R}$ associated with component failures have exponential distributions in which the parameters $\lambda(i,\ell)$ depend on the adjoining states i and ℓ and the response times $T(i,\ell)$, $\ell \in R$ have distributions $G(x;i,\ell)$, $\ell \in R$ with unspecified form.

One question that arises is whether any generality is added by permitting dependent response times. Results given by Miller, 1977, and Tsiatis, 1975, show that if $Q(x;i,j)$ is continuous, then independent random variables $\{T(i,\ell)\}$ exist having distributions that satisfy equation (1). In particular, when $Q(x;i,j)$ is continuous, the distributions of response times that satisfy equation (1) have survivor functions given by Tsiatis, 1975, as follows:

$$\bar{G}(x;i,j) = \exp\left\{-\int_0^x h(y;i,j)\, dy\right\}$$

where

$$h(y;i,j) = \theta(i,j)\, dQ(y;i,j) / \Sigma_{\ell \in R}\, \theta(i,\ell)\{1 - Q(y;i,\ell)\}$$

Thus, it suffices to consider only the representation given by equation (1).

3. GENERAL FORM OF THE BOUNDS

As the model now stands, we have not included an expected large difference in the component failure and system response times. Fault-tolerant systems often employ highly reliable components and are designed for quick response to component failures; hence, the response times may often be stochastically much smaller than

failure times. This assumption is the basis for the computational techniques proposed by Stiffler et al., 1979, and it is also the basis for the accuracy but not for the validity of the bounds given in the following discussion.

Our derivation, similar to that given by White, 1984, consists, in parts of partitioning a particular event series $z_0, z_1, \ldots, z_n$ according to the character of the potential sojourn times attached to $z_0, z_1, \ldots, z_{n-1}$. If $i \neq j$ and if all potential sojourn times attached to z_{i-1} correspond to component failures, while those attached to z_{j-1} include one or more system response times, then U_j is stochastically smaller than U_i, providing, of course, that the potential response times are stochastically smaller than the potential failure times. The upper bound is obtained by excluding the stochastically smaller random variables from the hitting time, $T = U_1 + U_2 + \ldots + U_n$, of z_n; thus, T is approximated by a sum of fewer variables. The lower bound is obtained in a similar way except that certain constants, chosen to represent upper percentiles of the response time distributions, replace the previously excluded variables; this gives a new random variable that, effectively, is stochastically larger than T.

Let $z_0, z_1, \ldots, z_n$ represent a particular path leading to an absorbing state z_n. Let A, B, and C partition the indices of $z_0, z_1, \ldots, z_n$ in the following way: $i \in A$ if all potential sojourn times leading from z_{i-1} represent elapsed times to component failures; $i \in B$ if the particular potential sojourn time leading from z_{i-1} to z_i represents a response time; and $i \in C$ provided that $i \notin A$ and the particular potential sojourn time leading from z_{i-1} to z_i represents an elapsed time to some component failure.

The probability $p(t)$ of hitting z_n by time t and entering the series of states $z_0, z_1, \ldots, z_n$ is

$$p(t) = P(T \leqq t, Z_0 = z_0, \ldots, Z_n = z_n)$$

where $T = U_1 + \ldots + U_n$ is the hitting time of z_n. This probability is given by

$$P(t) = \int_S \theta(z_0) \prod_{i=1}^{n} \theta(z_{i-1}, z_i)\, dQ(u_i; z_{i-1}, z_i) \qquad (2)$$

where

$$S = \{(u_1, u_2, \ldots, u_n): \; u_1 + u_2 + \ldots + u_n \leqq t\}$$

Let $\bar{\Delta} = \Sigma\Delta_i$ denote the sum of an arbitrarily chosen set of nonnegative constants Δ_i, $i \in BUC$. Upper and lower bounds $p_U(t)$ and $p_L(t)$, respectively, for $p(t)$ follow by observing, as in White, 1984, that the sets

$$S_U = \{(u_1, \ldots, u_n): \; \Sigma_A u_i \leqq t\}$$

and

$$S_L = \{(u_1, \ldots, u_n): \ \Sigma_A u_i \leqq t - \bar{\Delta},\ u_i \leqq \Delta_i,\ i \in BUC\}$$

satisfy $S_L \subseteq S \subseteq S_U$.

Now, replacing S by S_U and S_L in equation (2) gives, respectively,

$$P_U(t) = \theta(z_0)\ H(t)\ \Pi_A\ a_i\ \Pi_B\ b_i\ \Pi_C\ c_i \tag{3}$$

and

$$P_L(t) = \theta(z_0)\ H(t - \bar{\Delta})\ \Pi_A\ a_i\ \Pi_B\ b_i'\ \Pi_C\ c_i' \tag{4}$$

where, in terms of $\lambda_i = \Sigma_{\ell \in \bar{R}}\ \lambda(i, \ell)$,

$$a_i = \lambda(z_{i-1}, z_i)/\lambda_i \tag{5}$$

$$b_i = \int_0^\infty e^{-\lambda_i y}\ \Pi_{\ell \neq z_i}\ \bar{G}(y; z_{i-1}, \ell)\ dG(y; z_{i-1}, z_i) \tag{6}$$

$$c_i = \int_0^\infty e^{-\lambda_i y}\ \lambda(z_{i-1}, z_i)\ \Pi_\ell\ \bar{G}(y; z_{i-1}, \ell)\ dy \tag{7}$$

$$b_i' = \int_0^{\Delta_i} e^{-\lambda_i y}\ \Pi_{\ell \neq z_i}\ \bar{G}(y; z_{i-1}, \ell)\ dG(y; z_{i-1}, z_i) \tag{8}$$

$$c_i' = \int_0^{\Delta_i} e^{-\lambda_i y}\ \lambda(z_{i-1}, z_i)\ \Pi_\ell\ \bar{G}(y; z_{i-1}, \ell)\ dy \tag{9}$$

The function

$$H(x) = P(\Sigma_A U_i \leqq x) \tag{10}$$

appearing in equations (3) and (4) represents the distribution function for a sum of independent random variables having exponential distributions with rate parameters

λ_i, $i \in A$. The indices for each product shown in equations (6) to (9) vary only over the indices of the response time distributions.

The quantities b_i, c_i, b_i', and c_i' are directly estimable whenever the response times are observed experimentally. The choice of estimates would vary depending on whether the response times are observed individually or observed as competing events. In the former case, substitution of censored data forms of the sample cumulative distributions would give nonparametric estimates. In the latter case, nonparametric estimates as described by Kalbfleisch and Prentice, 1980, would be applicable. The Δ_i would probably be chosen as points of censoring, hopefully at the extreme upper tails of the response time distributions.

4. BOUNDS EXPRESSED IN TERMS OF TRANSITION PROBABILITIES, CONDITIONAL MEANS, AND PERCENTILES

One application of the bounds given earlier assumes that component failure rates are known quantities and that certain minimal information is available concerning the distributions of response times. In White, 1984, the model is limited to the case in which a single response time is competing with component failures and the bounds are given in terms of means and variances. For the general case, it is unlikely that accurate bounds can be expressed solely in terms of means and variances. The upper bounds given in this section require only information concerning certain transition probabilities and percentiles. The lower bounds require additional information concerning the conditional mean minimum response times.

Consider first the upper bound given by equation (3). Since typically the rate parameters $\lambda(i,j)$ take quite small values, a fairly accurate upper bound is given by replacing b_i and c_i appearing in equation (3) by

$$b_{1i} = \int_0^\infty \Pi_{\ell \neq z_i} \bar{G}(y; z_{i-1}, \ell)\, dG(y; z_{i-1}, z_i) \tag{11}$$

$$c_{1i} = \lambda(z_{i-1}, z_i)\, G_i(\Delta_i)\, \mu_i(\Delta_i) + \Delta_i\, \lambda(z_{i-1}, z_i)\, \bar{G}_i(\Delta_i) + \lambda(z_{i-1}, z_i)\, \bar{G}_i(\Delta_i)\, \lambda_i^{-1} \tag{12}$$

where

$$\bar{G}_i(\Delta_i) = \Pi_\ell\, \bar{G}(\Delta_i; z_{i-1}, \ell) \tag{13}$$

$$G_i(\Delta_i) = 1 - \bar{G}_i(\Delta_i) \tag{14}$$

$$\mu_i(\Delta_i) = [G_i(\Delta_i)]^{-1} \int_0^{\Delta_i} x\, dG_i(x) \tag{15}$$

Note that each b_{1i} represents a transition probability and is computed as if all component failure modes were eliminated at state z_{i-1}. The b_{1i} takes a value equal to 1 whenever a single response time is competing with failure times. The quantity $\mu_i(\Delta_i)$ represents the conditional mean minimum response time given that the smallest response occurs in $(0,\Delta_i)$. Since $G_i(\Delta_i)\ \mu_i(\Delta_i) \leqq G_i(\Delta_i)\ \Delta_i$, the upper bound can be computed without knowledge of $\mu_i(\Delta_i)$. In this case the information needed to compute the upper bound consists of the transition probabilities and the probability that the smallest response time exceeds Δ_i.

Next, a new lower bound is given by replacing each of b_i' and c_i', appearing in equation (4) by the quantities

$$b_{1i}' = \exp(-\lambda_i \Delta_i)\ \{b_{1i} - \bar{G}_i(\Delta_i)\} \tag{16}$$

and

$$c_{1i}' = \lambda(z_{i-1},z_i)\ \exp(-\lambda_i \Delta_i)\ \{G_i(\Delta_i)\ \mu_i(\Delta_i) + \Delta_i\ \bar{G}_i(\Delta_i)\} \tag{17}$$

An optimal choice of the Δ_i to minimize $P_u(t) - P_L(t)$ would probably require some knowledge of the form of the distributions of response times. The simple results, $b_{1i} - b_{1i}' \leqq \lambda_i \Delta_i + \bar{G}_i(\Delta_i)$ and $c_{1i} - c_{1i}' \leqq \lambda_i^2 \Delta_i^2 + \bar{G}_i(\Delta_i)$, show that $b_{1i} - b_{1i}'$ and $c_{1i} - c_{1i}'$ each converge to 0 as λ_i and $\bar{G}_i(\Delta_i)$ decrease to 0. Also, with r representing the number of terms in $\Sigma_A U_i$, it is not difficult to show that $H(t) - H(t - \bar{\Delta})$ is dominated by $\{t^r - (t - \bar{\Delta})^r\}\ \Pi_A \lambda_i$.

This analysis suggests that if the system components are highly reliable and if the system is designed for quick response to component failures, then tight bounds would often be given by choosing Δ_i equal to large percentiles of the distributions of minimum response times. Exact methods for computing $H(x)$ are available in several introductory-level texts that discuss time homogeneous Markov processes.

5. BOUNDS EXPRESSED IN TERMS OF PERCENTILES AND CONDITIONAL MEANS

The bounds given in this section rely on weak assumptions relating the response time distributions. The aim is to reduce the information needed to compute the bounds. This is done by replacing b_{1i} appearing in equations (11) and (16) by other quantities, depending on the percentiles of the response time distributions.

Let $F(\cdot)$ represent a continuous baseline distribution and let C_1 denote the class of continuous distributions generated by $F(\cdot)$ in the following way: $G(\cdot)$ belongs to C_1 if $\bar{G}(x) = \{\bar{F}(x)\}^\alpha$ from some value of $\alpha > 0$ and all values of $x \geqq 0$. The class C_1 is often described as the class of distributions having proportional hazard rates. The class is nonparametric in the sense that it involves an unspecified form of a baseline distribution. It has been studied extensively (Kalbfleisch and Prentice, 1980) as a framework for developing nonparametric statistical methods.

In the present context, suppose that the response time distributions belong to C_1 for some unspecified baseline distribution. Then, each survivor function has the representation

$$\bar{G}(x;z_{i-1},\ell) = \{\bar{G}_i(x)\}^{\phi(z_{i-1},\ell)} \tag{18}$$

where

$$0 < \phi(z_{i-1},\ell) < 1$$

$$\Sigma_\ell\ \phi(z_{i-1},\ell) = 1$$

The survivor function for the minimum response time is given by

$$\bar{G}_i(x) = \Pi_\ell\ \bar{G}(x;z_{i-1},\ell) \tag{19}$$

Upon replacing b_{1i} appearing in equations (11) and (16) by

$$b_{1i} = \phi(z_{i-1},z_i)$$

$$= \left[\log \bar{G}(\Delta_i;z_{i-1},z_i)\right] \Big/ \left[\Sigma_\ell \log \bar{G}(\Delta_i;z_{i-1},\ell)\right] \tag{20}$$

we get upper bounds that require only information concerning the probabilities that the response times exceed Δ_i. The lower bounds still depend on the conditional mean minimum response time.

Now consider a second class C_2, generated from a continuous baseline distribution $F(\cdot)$ in the following way: $G(\cdot)$ belongs to C_2 if $G(x) = F^\alpha(x)$ for some value of $\alpha > 0$ and all values of $x \geqq 0$. This class is also nonparametric in the same sense as before; however, it appears to have been studied less as a basis for nonparametric inference.

If the response time distributions belong to C_2 for some unspecified baseline distribution, then each has the representation

$$G(x;z_{i-1},\ell) = \{H_i(x)\}^{\psi(z_{i-1},\ell)} \tag{21}$$

where

$$\left.\begin{aligned} 0 < \psi(z_{i-1}, \ell) < 1 \\ \Sigma_\ell \ \psi(z_{i-1}, \ell) = 1 \end{aligned}\right\} \tag{22}$$

The distribution function for the largest of the response times is given by

$$H_i(x) = \Pi_\ell \ G(x; z_{i-1}, \ell)$$

Substituting from equation (21) gives

$$b_{1i} = \int_0^1 \Pi_{\ell \neq z_i} \left\{ 1 - u^{\psi(z_{i-1}, \ell)} \right\} \psi(z_{i-1}, z_i) \ u^{\psi(z_{i-1}, z_i) - 1} \ du \tag{23}$$

Upon expanding the product in the integrand, b_{1i} can be written as a sum of terms involving only the quantities $\psi(z_{i-1}, \ell)$. Also, from equation (21) each $\psi(z_{i-1}, \ell)$ can be represented in the form

$$\psi(z_{i-1}, \ell) = \left[\log G(\Delta_i; z_{i-1}, \ell)\right] / \left[\Sigma_\ell \log G(\Delta_i; z_{i-1}, \ell)\right] \tag{24}$$

Therefore, b_{1i} as given by equations (23) and (24) depends only on the percentiles of the response time distributions and can be substituted in equations (11) and (16) to give a new set of bounds.

6. AN EXAMPLE

The example to be discussed is concerned with the effect on system reliability of a particular choice of interval for cycling a spare and serves to illustrate the application of the bounds given in section 4.

Consider a system having three active processor units and one spare. Active units have a failure rate λ and the spare has a failure rate μ. The output of the active units is subject to majority vote; thus, the system survives with one failed active unit. The spare and one predesignated active unit form a cooperating pair. To check its operational status, the spare is automatically activated and switched with the cooperating unit at regular intervals. The spare is also activated whenever a failed unit is detected and, in this case, it replaces the failed unit.

The desire to check the operational status of the spare leaves open the possibility of cycling in a failed spare at some instant when a noncooperating unit has failed. As shown in figure 1, one of the noncooperating active units fails (state 1), the spare fails (state 2), and the system, being unaware that either unit

has failed, automatically switches the spare with the good active unit (state 3). State 3, as well as states 5 and 7, represents system failure since the system is not fault tolerant at any instant when two of the three active units have failed. States 6 and 8 designate operational states that are attained when the system detects, identifies, and retires the failed active unit and then replaces it with the spare.

In terms of the previous notation, $z_0 = 0$, $z_1 = 1$, $z_2 = 2$, $z_3 = 3$, $A = \{1\}$, $B = \{3\}$, and $C = \{2\}$. For the sake of simplicity, take $\Delta_i = \Delta$ and assume that the response time distributions $G(x;1,6)$ and $G(x;2,8)$ are identical. The time (measured from the instant of entering state 2) needed to switch the spare to active status has a distribution limited to $(0,\Delta)$; that is, Δ is chosen equal to the length of the cycling interval and $\bar{G}(\Delta;2,3) = 0$.

The bounds have the form

$$P_U(t) = H(t)\ a_1 b_{13} c_{12}$$

and

$$P_L(t) = H(t - \bar{\Delta})\ a_1 b'_{13} c'_{12}$$

where $a_1 = 2\lambda(3\lambda + \mu)^{-1}$, $\bar{\Delta} = 2\Delta$, $H(x) = 1 - \exp\{-(3\lambda + \mu)x\}$, and b_{13}, c_{12}, b'_{13}, and c'_{12} are given by equations (11), (12), (16), and (17), respectively:

$$b_{13} = \int_0^\infty \bar{G}(x;2,8)\ dG(x;2,3)$$

$$c_{12} = \mu\{G_2(\Delta)\ \mu_2(\Delta) + \Delta\bar{G}_2(\Delta)\} + \mu(2\lambda + \mu)^{-1}\ \bar{G}_2(\Delta)$$

$$b'_{13} = \{b_{13} - \bar{G}_3(\Delta)\}\ \exp(-2\lambda\Delta)$$

$$c'_{12} = \mu\{G_2(\Delta)\ \mu_2(\Delta) + \Delta\bar{G}_2(\Delta)\}\ \exp[-(2\lambda + \mu)\Delta]$$

To compare the upper and lower bounds for the probability of hitting state 3 prior to completing the mission in 1 hr ($t = 1$), suppose that $\Delta = 0.003$, $\mu = \lambda = 0.001$, and experimental results give $\bar{G}(\Delta;1,6) = 0.04$, $\mu_2(\Delta) = 0.002$, and $b_{13} = 0.68$. Then, $\bar{G}_2(\Delta) = 0.04$, $\bar{G}_3(\Delta) = 0$, and upper and lower bounds are $P_U(t) = 1.81 \times 10^{-5}$ and $P_L(t) = 2.74 \times 10^{-9}$, respectively.

The difference between the upper and lower bounds is largely due to the difference in c_{12} and c'_{12}, but this in turn can be attributed to a lack of information concerning the shapes of the distributions above the limit Δ.

If it is assumed that $G(x;2,3)$ is a uniform distribution over $(0,\Delta)$, then less information is needed to compute the bounds; in this case,

$$b_{13} = \Delta^{-1} \int_0^{\Delta} \bar{G}(x;2,3)\, dx = \Delta^{-1}\{G_2(\Delta)\ \mu_2(\Delta) + \Delta\ \bar{G}_2(\Delta)\}$$

and substitution gives $b_{13} = 0.68$.

CONCLUDING REMARKS

In this paper a semi-Markov model has been analyzed to give upper and lower bounds for system unreliability. The model provides for multiple competing system responses to component failures and is flexible in terms of describing the distributions of system response times. We have shown that accuracy of the bounds increases in the limit as the component failure rates and as the survivor functions of minimum response times decrease to 0. Thus, generally if the response time distributions are concentrated over a narrow range, accurate bounds would be given by selecting percentiles at the upper end of this range. The best choice of parameters for representing the bounds depends on the available information; in the experimental context, percentiles and conditional means appear preferable to other parameters because of the ease of substituting censoring points for percentiles and the ease of directly estimating the conditional mean response times.

NASA Langley Research Center
Hampton, VA 23665
December 17, 1984

REFERENCES

Geist, Robert M.; and Trivedi, Kishor S. 1983: Ultrahigh Reliability Prediction in Fault-Tolerant Computer Systems. IEEE Trans. Comput., C-32, no. 12, Dec., pp. 1118-1127.

Kalbfleisch, J. D.; and Prentice, R. L. 1980: The Statistical Analysis of Failure Time Data. John Wiley & Sons.

Lagakos, S. W.; Sommer, C. J.; and Zelen, M. 1978: Semi-Markov Models for Partially Censored Data. Biometrika, vol. 65, no. 2, pp. 311-317.

Lala, Jaynarayan H.; and Smith, T. Basil, III. 1983: Development and Evaluation of a Fault-Tolerant Multiprocessor (FTMP) Computer, Volume III - FTMP Test and Evaluation. NASA CR-166073.

Miller, Douglas R. 1977: A Note on Independence of Multivariate Lifetimes in Competing Risk Models. Ann. Statist., vol. 5, no. 3, pp. 576-579.

Montgomery, Raymond C. 1975: Failure Detection and Control-System Reconfiguration: Past, Present, and Future. Systems Reliability Issues for Future Aircraft, NASA CP-003, pp. 69-78.

Ng, Ying-Wah; and Avižienis, Algirdas. 1976: A Model for Transient and Permanent Fault Recovery in Closed Fault-Tolerant Systems. Proceedings - 1976 International Symposium on Fault-Tolerant Computing, IEEE, pp. 182-188.

Smith, T. B.; Hopkins, A. L.; Hall, E. C.; Howatt, J. R.; and Lala, J. H. 1977: A Fault-Tolerant Multiprocessor Architecture for Aircraft - Volume II. Contract NAS1-13782, Charles Stark Draper Lab., Inc., Apr. (Available as NASA CR-165915.)

Stiffler, J. J.; Bryant, L. A.; and Guccione, L. 1979: CARE III Final Report, Phase I, Volume I. NASA CR-159122.

Tsiatis, Anastasios. 1975: A Nonidentifiability Aspect of the Problem of Competing Risks. Proc. Nat. Acad. Sci. U.S.A., vol. 72, no. 1, Jan., pp. 20-22.

Walker, Bruce K. 1980: A Semi-Markov Approach to Quantifying Fault-Tolerant System Performance. Ph.D. Thesis, Massachusetts Inst. of Technol., July.

White, Allen L. 1984: Upper and Lower Bounds for Semi-Markov Reliability Models of Reconfigurable Systems. NASA CR-172340.

Willsky, Alan S. 1976: A Survey of Design Methods for Failure Detection in Dynamic Systems. Automatica, vol. 12, no. 6, Nov., pp. 601-611.

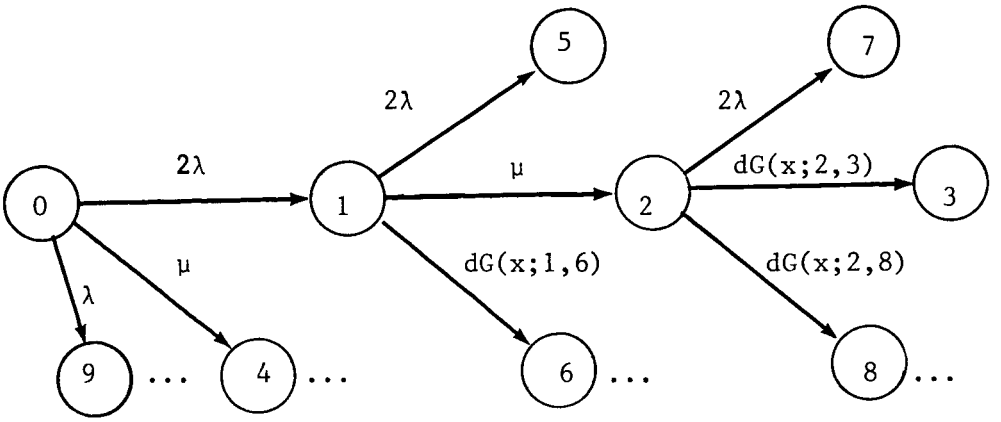

Figure 1.- State diagram for an example system consisting of three active processor units and one spare.

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
NASA TP-2409		

4. Title and Subtitle	5. Report Date
RELIABILITY BOUNDS FOR FAULT-TOLERANT SYSTEMS WITH COMPETING RESPONSES TO COMPONENT FAILURES	April 1985
	6. Performing Organization Code: 505-34-13-30
7. Author(s): Larry D. Lee	8. Performing Organization Report No.: L-15853
	10. Work Unit No.
9. Performing Organization Name and Address: NASA Langley Research Center, Hampton, VA 23665	11. Contract or Grant No.
	13. Type of Report and Period Covered: Technical Paper
12. Sponsoring Agency Name and Address: National Aeronautics and Space Administration, Washington, DC 20546	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This paper establishes bounds on the probability of system failure for fault-tolerant systems of the type used, for example, in aviation control. Event series leading to system failure are assumed to follow a semi-Markov model in which the potential sojourn times associated with component failures have exponential distributions and those associated with system responses have distributions with unspecified form. A product form of the bounds is derived by using a model that provides for multiple competing system responses to component failures.

17. Key Words (Suggested by Author(s))	18. Distribution Statement
Fault-tolerant systems Semi-Markov model Reliability bounds Competing system responses	Unclassified - Unlimited Subject Categories 38, 59, and 65

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	14	A01

For sale by the National Technical Information Service, Springfield, Virginia 22161 NASA-Langley, 1985

National Aeronautics and
Space Administration

Washington, D.C.
20546

Official Business
Penalty for Private Use, $300

THIRD-CLASS BULK RATE

Postage and Fees Paid
National Aeronautics and
Space Administration
NASA-451

1 2 1U,D,G, 850329 S00161DS
DEPT OF THE AIR FORCE
ARNOLD ENG DEVELOPMENT CENTER(AFSC)
ATTN: LIBRARY/DOCUMENTS
ARNOLD AF STA TN 37389

NASA

POSTMASTER: If Undeliverable (Section 158 Postal Manual) Do Not Return